The Brill-Segre formula and the *abc* conjecture

José Felipe Voloch

This is a write-up of lectures presented at the first Arizona Winter School in Arithmetic Geometry on the *abc* conjecture. There isn't anything new in these notes, except perhaps the point of view. Most of the results are in [V] and [TV].

The Brill-Segre formula counts the number of osculation points for a morphism of a curve to n-dimensional space and generalizes the Hurwitz formula ($n = 1$) and the Plucker formula ($n = 2$). The Brill-Segre formula implies the *abc* theorem for function fields for arbitrarily many summands. Smirnov has suggested a conjectural analogue of Hurwitz formula for number fields which implies the *abc* conjecture. We had hoped to be able to formulate a corresponding number field analogue of the Brill-Segre formula, but had to stop short of that goal and discuss only local aspects of such an analogue.

Let X be an irreducible, nonsingular, projective algebraic curve of genus g defined over an algebraically closed field k of **characteristic zero** (see the papers of J. Wang [W1,2] for the case of positive characteristic). Let K be the function field of X. For elements $f_0, \dots, f_n$ of K, not all zero, we define the height as

$$h(f_0, \dots, f_n) := \sum_{P \in X} - \min\{v_P(f_0), \dots, v_P(f_n)\},$$

where $v_P(f)$ is the order of f at a point P of X.

Let $f_0, \dots, f_n \in K$ and be linearly independent over k. Consider the morphism $\phi = (f_0, \dots, f_n) : X \to \mathbf{P}^n$. For each $P \in X$ we have

$$f(P) = ((t_P^{e_P} f_0)(P), \dots, (t_P^{e_P} f_n)(P))$$

where $e_P := -\min\{v_P(f_0), \dots, v_P(f_n)\}$ and t_P is a local parameter of X at P. The set $\{v_P(\sum_{i=0}^n a_i f_i) + e_P \mid a_i \in k\}$ consists of $n+1$ integers, say $0 \le j_0 < j_1 < \dots < j_n \le \deg \phi$, where $\deg \phi = h(f_0, \dots, f_n)$ is the degree of ϕ. This can be shown as follows. There is a descending sequence $\mathbf{P}^n = V_0 \supseteq V_1 \supseteq V_2 \supseteq \cdots$ of linear subspaces of $\mathbf{P}^n$ such that, for each $m \geq 0$

$$V_m(k) = \{(a_0 : \ldots : a_n) \in \mathbf{P}^n(k) \mid v_P(\sum_{i=1}^{n} a_i f_i) + e_P \geq m)\}.$$

Indeed, the condition in question amounts to m linear conditions on the indeterminate constants $a_1, \ldots, a_n$. Geometrically, we view $a_1, \ldots, a_n$ as the coordinates of the hyperplane $\sum a_i X_i = 0$ and interpret V_m as the space of hyperplanes in $\mathbf{P}^n$ which meet our curve with multiplicity at least m at P. At each stage $V_m = V_{m+1}$ or V_{m+1} is of codimension one in V_m. Also, it is clear that V_m is empty for m large, since the descending sequence $\mathbf{P}^n = V_0 \supseteq V_1 \supseteq V_2 \supseteq \cdots$ must stabilize and $\bigcap V_m = \emptyset$ since the f_i are linearly independent over k. Therefore there are exactly $n+1$ integers, say $0 \leq j_0 < j_1 < \ldots < j_n$ with $V_m = V_{m+1}$ if and only if $m \neq j_i$ for all i. In particular $\dim V_m = n - i$, for $j_{i-1} < m \leq j_i$.

Brill-Segre formula. *Let $\phi : X \to \mathbf{P}^n$ be a morphism. For each $P \in X$ define $w_\phi(P) = \sum_{i=0}^{n} (j_i - i)$, then $\sum_{P \in X} w_\phi(P) = n(n+1)(g-1) + (n+1)\deg \phi$.*

We will not give a proof of this result here since it is readily available in the literature, see, e.g., [FK],[GH],[SV], etc.

It follows from the Brill-Segre formula that there exists only finitely many points in X where $(j_0, \ldots, j_n) \neq (0, \ldots, n)$. These points are called the Weierstrass points for the morphism ϕ and $w_\phi(P)$ is called the weight of P.

We will now use the Brill-Segre formula to prove (see [BM] or [V]):

Theorem. *Suppose $u_1, \ldots, u_m \in K$ are linearly independent over k, satisfy $u_1 + \ldots + u_m = 1$ and let $S = \{P \in X \mid \exists i, v_P(u_i) \neq 0\}$ then:*

$$h(u_1, \ldots, u_m) \leq \frac{m(m-1)}{2}(2g - 2 + \#S).$$

This is a generalization of Mason's *abc* theorem which corresponds to $m = 2$. Before embarking on the proof (which will follow [V]) we need a lemma.

Lemma. *If $v_P(f_0) \leq v_P(f_1) \leq \ldots \leq v_P(f_n)$, then $j_i \geq v_P(f_i) + e_P$, for $i = 0, ..., n$.*

Proof: The hypothesis implies that the linear space $x_0 = \cdots = x_{i-1} = 0$ is contained in V_m, where $m = v_P(f_i) + e_P$, so $\dim V_m \geq n - i$. However, j_i is defined by $\dim V_{j_i} = n - i$ so $j_i \geq v_P(f_i) + e_P$, as desired.

Proof of the theorem: Consider the morphism $\phi : X \to \mathbf{P}^{m-1}$ given by $(u_1 : \ldots : u_m)$. Given a point $P \in X$, choose j such that $v_P(u_j) = -e_P$. We can make a change of coordinates that replaces u_j by $\sum u_i = 1$. After reordering the new coordinates we can assume we are under the hypotheses of the lemma and therefore

$$\sum j_i \geq v_P(1) + e_P + \sum_{i \neq j} (v_P(u_i) + e_P) = \sum_{i \neq j} v_P(u_i) + m e_P = \sum v_P(u_i) + (m+1) e_P.$$

So $w_\phi(P) = \sum j_i - m(m-1)/2 \geq \sum v_P(u_i) + (m+1)e_P - m(m-1)/2$. Thus

$$\sum_{P \in S} w_\phi(P) \geq \sum_{P \in S} (m+1)e_P - m(m-1)/2 + \sum_i v_P(u_i)$$

$$= (m+1) h(u_1, \ldots, u_m) - m(m-1)/2 |S|.$$

On the other hand, $\sum_{P \in S} w_\phi(P) \leq \sum_{P \in X} w_\phi(P) = m(m-1)(g-1) + m h(u_1, \ldots, u_m)$ by the Brill-Segre formula, and these two inequalities immmmmmediately give the theorem.

We will now consider an arithmetic analogue of the above. Let $a_1, \ldots, a_n$ be elements of a number field K. Thinking of K as the function field of a non-existent curve, $(a_1 : \ldots : a_n)$ can be viewed as a map of the curve to $\mathbf{P}^{n-1}$. This point of view has been dubbed "geometry over the field of one element" (see [M] or [Sm] and also [I], which is perhaps in the same spirit). We can consider the local and global aspects of the situation. In [Sm], Smirnov studies the case $n = 2$, where the local theory is trivial, and makes some global conjectures in the spirit of a number field analogue of the Hurwitz formula. He asks about a possible higher dimensional generalization of his conjecture, which should be an analogue of the Plücker formulas in dimension two which corresponds to $n = 3$, and their higher dimensional extensions, that is, the Brill-Segre formula. The results obtained in

[TV] provide a possible local theory towards such a generalization and the next step will be to formulate such a higher dimensional global conjecture.

Consider an unramified local field K of characteristic zero with perfect residue field k of characteristic $p > 0$, and $a_1, \ldots, a_n \in K$. As K has no constant field, we take as replacement the set of Teichmüller representatives of the elements of of k, which we denote by $T(k)$. Denote the valuation on K by $v(.)$.

Theorem ([TV]). *Let K be as above. Given $a_1, \ldots, a_n \in K$, there exists a positive integer m such that for $\zeta_1, \ldots, \zeta_n \in T(k)$, either $\sum \zeta_i a_i = 0$ or $v(\sum \zeta_i a_i) \leq m$.*

Proof: Without loss of generality, we can assume that k is algebraically closed and that $a_1, \ldots, a_n$ are in the ring of integers of k, which we can identify with the ring of Witt vectors of infinite length over k. For $z \in k$ we let $T(z)$ denote its Teichmüller representative $T(z) = (z, 0, 0, \ldots)$. Since the Witt vectors of length m form a ring scheme and T is multiplicative, the condition $\sum \zeta_i a_i \equiv 0 \pmod{p^m}$, for $\zeta_i = T(z_i)$, translates into a set of m homogeneous polynomial equations in $z_1, \ldots, z_n$ and therefore defines a closed subscheme V_m of $\mathbf{P}^{n-1}$ over k. Moreover, the V_m form a decreasing sequence, so must become constant. If $V_{m_0} = V_m$, for $m > m_0$, then any $\zeta_1, \ldots, \zeta_n \in T(k)$ whose residues $z_1, \ldots, z_n$ define a point in V_{m_0} satisfies $\sum \zeta_i a_i = 0$ and all others satisfy $v(\sum \zeta_i a_i) \leq m_0 - 1$. This completes the proof.

The V_m in the above proof are the analogues of the V_m in the function field case. In the function field case they were linear spaces, thus reduced, irreducible and equidimensional. In the arithmetic case they are just schemes which may not be reduced, irreducible or equidimensional. See [TV] for examples and for results that ensure that the V_m are well-behaved for small m.

Assume now we are dealing with the global situation. To begin with define the weight of a place w of K. A weak version is the following

$$M_w = \frac{1}{p^{(n-1)(n-2)/2}} \sum_{(z_1:\ldots:z_n) \in V_{n-1}} \big(w(\sum a_i T(z_i)) - (n-1)\big).$$

As a first approximation to the Brill-Segre formula one can ask if the infinite series $\sum_w M_w \log Nw$ converges if $n \geq 3$. There is no good reason to assume it is a finite sum, but the convergence seems reasonable. A formula, or at least an estimate, for the sum of this series would then be the required conjecture. One would like to add an archimedian term, as in [Sm], also. At this point, further theoretical work and numerical experimentation seem advisable before hazarding a shape for this formula. Such a formula should imply the generalized *abc*-conjecture for number fields with arbitrarily many summands, so it lies quite deep. Also, it should be mentioned that in [SV] we obtain a variant of the Brill-Segre formula "twisted by Frobenius" that leads to a proof of the Riemann hypothesis for function fields and one may speculate whether there is something similar in the number field case. Like in [Sm], such a conjecture would have implications to some classical arithmetic questions such as whether there are infinitely many primes satisfying $a^{p-1} \equiv 1 \pmod{p^2}$ or $(\bmod\, p^3)$, where a is some fixed integer.

Acknowledgements: The NSF GIG grant provided support for my attendance at the meeting and for the meeting itself. I would also like to acknowledge financial support from the NSA (grant MDA904-97-1-0037). I'd like to thank Jeff Lagarias for lending me the notes he took during my lectures which were very useful in the preparation of these notes and Jaap Top who corrected some mistakes in an earlier version of these notes.

References.

[BM]W. D. Brownawell and D. W. Masser, Vanishing sums in function fields, Math. Proc. Cambridge Philos. Soc. 100 (1986), no. 3, 427–434]

[FK] H. Farkas and I. Kra, Riemann surfaces, Springer GTM.

[GH] P. Griffiths and J. Harris, Principles of Algebraic Geometry, Wiley.

[M] Mason, R. C. Diophantine equations over function fields. London Mathematical Society Lecture Note Series, 96. Cambridge University Press, Cambridge-New York, 1984.

[Si] Silverman, J. H. The S-unit equation over function fields. Math. Proc. Cambridge Philos. Soc. 95 (1984), no. 1, 3–4

[Sm] Smirnov, A. L. Hurwitz inequalities for number fields. (Russian) Algebra i Analiz 4 (1992), no. 2, 186–209; translation in St. Petersburg Math. J. 4 (1993), no. 2, 357–37

[SV] Stöhr, K-O. and Voloch, J.F. Weierstrass Points and Curve over Function Fields Proc. London Math. Soc.(3) vol 52 1986 1–19

[TV] Tate, J. and Voloch, J. F., Linear forms in p-adic roots of unity. Internat. Math. Res. Notices

[V] Voloch, J. F., Diagonal equations over function fields. Bol. Soc. Brasil. Mat. 16 (1985), no. 2, 29–39

[W] Wang, J, T.-Y., The Truncated Second Main Theorem of Function Fields, J. Number Theory 58 (1996) 139-157.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu